



guida di desktop management

workstation hp xw4000

workstation hp xw6000

Numero di parte del documento: 301201-061

Ottobre 2002

La presente guida fornisce definizioni ed istruzioni delle funzioni di sicurezza d'uso e Intelligent Manageability preinstallate su alcuni modelli.

© 2002 Hewlett-Packard Company

Compaq, il logo Compaq, ROMPaq e iPAQ sono marchi di Compaq Information Technologies Group, L.P. negli USA e/o in altri paesi.

Microsoft, MS-DOS, Windows e Windows NT sono marchi di Microsoft Corporation negli U.S.A. e/o in altri paesi.

Intel, Pentium, Intel Inside e Celeron sono marchi di Intel Corporation negli USA e/o in altri paesi.

I nomi di tutti gli altri prodotti citati nel presente documento possono essere marchi delle rispettive società.

Hewlett-Packard Company declina ogni responsabilità per errori od omissioni tecniche o editoriali contenuti in questa guida, per danni accidentali o consequenziali risultanti dalla fornitura, dalle prestazioni o dall'uso di questo materiale. Le informazioni contenute nel presente documento sono fornite nello stato in cui si trovano ("as is") senza garanzie di nessun tipo comprese, senz'intento limitativo, garanzie implicite di commerciabilità idoneità per scopi specifici e sono soggette a variazioni senza preavviso. Le garanzie sui prodotti HP sono definite nei certificati di garanzia allegati ai prodotti. Nulla di quanto qui contenuto potrà essere interpretato nel senso della costituzione di una garanzia aggiuntiva.

Il presente documento contiene informazioni proprietarie protette da copyright. Nessuna parte del documento può essere fotocopiata, riprodotta o tradotta in altra lingua senza la preventiva autorizzazione scritta di Hewlett-Packard Company.



AVVERTENZA: Il testo presentato in questo modo indica che la mancata osservanza delle istruzioni potrebbe comportare lesioni fisiche o addirittura la perdita della vita.



ATTENZIONE: Il testo presentato in questo modo indica che la mancata esecuzione delle indicazioni fornite potrebbe provocare danni all'apparecchiatura o la perdita di informazioni.

guida di desktop management

workstation hp xw4000

workstation hp xw6000

Prima edizione (Ottobre 2002)

Numero di parte del documento: 301201-061

Sommario

Guida di Desktop Management

Configurazione iniziale e deployment.	2
Installazione remota del sistema	3
Gestione e aggiornamento del software	3
Altiris eXpress	4
Altiris eXpress PC Transplant Pro	6
Altiris eXpress HP/Compaq Client Manager	6
System Software Manager	7
Product Change Notification	7
ActiveUpdate	7
Flash della ROM	8
Flash remoto della ROM.	8
ROM con blocco di avviamento FailSafe.	9
Replica delle impostazioni	11
Pulsante d'accensione bistabile	11
Gestione dell'alimentazione	12
Sito World Wide Web.	13
Moduli e collaboratori.	13
Interfaccia di gestione del desktop (DMI)	14
Wired for Management.	14
Controllo e sicurezza delle risorse.	15
Sicurezza tramite password	18
Cancellazione delle password di accensione e di configurazione	23
Modalità server di rete	24
DriveLock	24
Sensore Smart Cover	27
chiusura Smart Cover	28
Master Boot Record Security (Sicurezza MBR).	31
Predisposizione per chiusura con cavo	34
Tecnologia per l'identificazione delle impronte digitali.	34

Notifica guasti e ripristino.	34
Drive Protection System (DPS)	35
Monitoraggio dell'integrità ultra ata.	35
Alimentatore protetto contro gli sbalzi di tensione.	35
Sensore termico.	35

Indice Analitico

Guida di Desktop Management

HP propone soluzioni per la gestione dei desktop fin dal 1995, con l'introduzione sul mercato dei primi personal computer completamente gestibili. Da allora HP ha condotto un incessante sforzo per sviluppare gli standard e le infrastrutture occorrenti per il deployment, la configurazione e la gestione efficaci di PC desktop, workstation e portatili. HP Intelligent Manageability fornisce soluzioni standard per la gestione ed il controllo di PC desktop, workstation e portatili in ambienti di rete. HP collabora con le principali case produttrici di soluzioni software di gestione oggi sul mercato, con l'obiettivo di assicurare la necessaria compatibilità tra la Gestione intelligente e tali prodotti. Intelligent Manageability è un elemento importante del grande impegno che HP ha posto nella realizzazione di soluzioni relative al ciclo vitale del PC, in grado di seguire l'utente nelle quattro fasi della pianificazione, deployment, gestione e transizioni.

Questa guida riassume le capacità e le caratteristiche dei sette componenti chiave della Gestione del desktop:

- Initial configuration and deployment (Configurazione iniziale e installazione)
- Remote system installation (Installazione remota del sistema)
- Software updating and management (Aggiornamento e gestione del software)
- ROM flash (Flash della ROM)
- Building blocks and partners (Moduli e collaboratori)
- Asset tracking and security (Controllo e sicurezza delle risorse)
- Fault notification and recovery (Notifica guasti e ripristino)



Il supporto di funzioni specifiche descritte in questa guida può variare in base al modello e alla versione del software.

Configurazione iniziale e deployment

Il computer viene fornito con un'immagine software di sistema preinstallata. Dopo una velocissima fase di “scompattamento” del software il computer è pronto per l'uso.

Potrebbe rivelarsi necessario sostituire l'immagine del software preinstallata con un set personalizzato di software applicativi e di sistema. In tal caso, esistono vari metodi per personalizzare il software. È possibile operare come segue:

- Installare il software applicativo aggiuntivo dopo aver scompattato l'immagine del software preinstallata.
- Utilizzare strumenti di installazione come Altiris eXpress, Microsoft MS Batch o Microsoft NT Distribution Share (NTDS) per sostituire il software preinstallato con un'immagine del software personalizzata.
- Eseguire una procedura di clonazione del disco per copiare il contenuto da un disco fisso ad un altro.

Il metodo di messa in uso da scegliere dipende dai processi e dagli ambienti informatici degli utenti. La sezione PC Deployment (Installazione del PC) del sito Web Solutions and Services (Soluzioni e Servizi) (<http://www.compaq.com/solutions/pcsolutions>) fornisce informazioni utili per la scelta del metodo migliore di installazione. Sul sito si trovano anche guide ed utility da integrare con gli strumenti di deployment basati su Microsoft o PXE.

I CD *Compaq Restore* (o *Restore Plus!*), l'installazione da ROM e l'hardware compatibile ACPI forniscono ulteriore assistenza per il ripristino del software di sistema, la gestione e la soluzione dei problemi di configurazione e la gestione dell'alimentazione.

Installazione remota del sistema

L'installazione remota del sistema consente di avviare e impostare il proprio sistema utilizzando il software e le informazioni di configurazione situati in un server di rete. La funzione di installazione remota del sistema viene di solito utilizzata come strumento di impostazione e configurazione del sistema e può servire ai seguenti scopi:

- Installazione di una copia del software su uno o più PC nuovi.
- Formattazione di un disco fisso.
- Installazione di software applicativo o di driver per applicazioni.
- Aggiornamento del sistema operativo, del software di applicazione o dei driver.

Per avviare l'installazione remota del sistema premere **F12** quando viene visualizzato il messaggio F12 = Avvio servizio di rete nell'angolo inferiore sinistro della schermata del logo HP. Per proseguire seguire le istruzioni sullo schermo.

HP e Altiris, Inc. si sono associati per poter fornire strumenti progettati per facilitare il compito di unire installazione e gestione del PC con meno dispendio di tempo, riducendo infine i costi totali di proprietà e rendendo i PC HP i più gestibili PC client nell'ambiente aziendale.

Gestione e aggiornamento del software

HP ha dotato desktop e workstation di diversi strumenti per la gestione e l'aggiornamento del software, Altiris eXpress, Altiris eXpress PC Transplant Pro, Altiris eXpress HP/Compaq Client Manager, System Software Manager, Product Change Notification ed Active Update.

Altiris eXpress

HP ed Altiris hanno esteso la partnership a soluzioni leader a livello industriale che riducono la complessità di gestione hardware e software per desktop, portatili, dispositivi palmari e server per tutto la loro durata. Altiris eXpress consente all'amministratore del sistema di creare e di installare in poco tempo un'immagine del software standard aziendale e personalizzata su uno o più PC client in rete con un'interfaccia semplice da utilizzare come Windows Explorer. Altiris eXpress supporta Wired for Management e Preboot Execution Environment (PXE) di Intel. Con Altiris eXpress e le funzioni d'installazione remota del sistema del computer HP non è necessario che l'amministratore si rechi personalmente presso ogni nuovo PC per scompattare la copia del software.

Le soluzioni Altiris eXpress costituiscono un modo efficace e funzionale per automatizzare i processi esistenti e risolvere le zone problematiche nell'ambiente informatico in uso. Con un'infrastruttura di tipo Web Altiris eXpress è in grado di gestire i sistemi da qualunque luogo e in qualsiasi momento, anche da un PC iPAQ Pocket.

Le soluzioni Altiris eXpress sono modulari ed estendibili per soddisfare le esigenze a livello di workgroup e di aziende e si integrano con altri strumenti di gestione client, fornendo estensioni a Microsoft BackOffice/SMS.

Le soluzioni Altiris eXpress espanse riguardano quattro aree informatiche fondamentali:

- Installazione e migrazione
- Gestione software e operativa
- Gestione componenti hardware e risorse
- Help Desk e risoluzione dei problemi

Nel giro di pochi minuti dall'installazione Altiris eXpress è in grado d'installare un'immagine disco contenente il sistema operativo, il software applicativo ed il client Altiris eXpress, senza bisogno di dischetti d'avvio. Con Altiris eXpress gli amministratori di rete possono:

- Creare una nuova immagine o modificarne una esistente, oppure clonare un PC in rete contenente l'immagine ideale.
- Creare qualsiasi numero di immagini disco personalizzate per numerosi gruppi di lavoro.
- Modificare i file d'immagine senza dover ripartire da zero. Ciò è reso possibile dal fatto che Altiris eXpress memorizza i file nel loro formato nativo: NTFS, FAT16 o FAT32.
- Stabilire un "New PC Event" (Nuovo evento PC), ovvero uno script da eseguire automaticamente quando viene aggiunto un PC in rete. Lo script può, ad esempio, formattare il disco fisso, effettuare il flash del BIOS su ROM ed installare un'immagine software standard completa.
- Programmare l'esecuzione di un evento su un gruppo di computer.

Altiris eXpress è anche dotato di funzioni di distribuzione software di facile uso. Altiris eXpress può essere utilizzato per aggiornare i sistemi operativi e il software di applicazione da una console centrale. In abbinamento a SSM, Altiris eXpress è anche in grado di aggiornare il BIOS su ROM e i driver di periferica.

Per ulteriori informazioni visitare
<http://www.compaq.com/easydeploy>.

Altiris eXpress PC Transplant Pro

Altiris eXpress PC Transplant Pro garantisce una migrazione indolore del PC mantenendo le vecchie impostazioni e preferenze e i vecchi dati e trasportandoli in modo semplice e rapido nel nuovo ambiente. L'upgrade richiede solo alcuni minuti, anziché ore o giorni, e il desktop e le applicazioni hanno l'aspetto e le funzioni previste.

Per ulteriori informazioni e particolari sulle modalità di download di una copia di valutazione valida 30 giorni completa di tutte le funzioni visitare <http://www.compaq.com/easydeploy>.

Altiris eXpress HP/Compaq Client Manager

Altiris eXpress HP/Compaq Client Manager integra a fondo la tecnologia HP Intelligent Manageability in Altiris eXpress per fornire funzioni di gestione hardware superiori per dispositivi d'accesso HP, fra cui:

- Elenchi dettagliate dei componenti hardware per la gestione delle risorse
- Monitoraggio e diagnostica dello stato del PC
- Notifica proattiva di modifiche nell'ambiente hardware
- Report accessibile da Web di particolari di estrema importanza come macchine con sistemi di allarmi di temperatura, di memoria ed altro ancora
- Aggiornamento a distanza di software di sistema, ad esempio driver e BIOS della ROM

Per ulteriori informazioni su Altiris eXpress HP/Compaq Client Manager visitare <http://www.compaq.com/easydeploy>.

System Software Manager

System Software Manager (SSM) è un'utility che consente di aggiornare il software a livello di sistema su più PC contemporaneamente. Se eseguita su un sistema client del PC, SSM rileva le versioni hardware e software, quindi aggiorna il software appropriato attingendo da un apposito archivio centrale. Le versioni dei driver supportati da SSM sono indicate con un'icona particolare nel sito Web dal quale scaricare i driver e sul CD del software di supporto. Per scaricare l'utility o per ulteriori informazioni su SSM visitare

<http://www.compaq.com/im/ssmwp.html>.

Product Change Notification

PCN è il programma di notifica modifiche al prodotto di HP che utilizza un sito Web sicuro in cui creare profili personalizzati che in modo proattivo ed automatico consentano di:

- Ricevere notifica tramite e-mail di modifiche hardware e software alla maggior parte di computer e server in commercio.
- Ricevere e-mail contenenti Customer Advisories per la maggior parte di computer e server in commercio.

Il sito Web PCN consente inoltre di cercare tutte le Product Change Notifications e Customer Advisories per la maggior parte di PC e server disponibili in commercio.

Per saperne di più su PCN e creare un profilo personalizzato visitare <http://www.compaq.com/pcn>.

ActiveUpdate

ActiveUpdate è un'applicazione HP di tipo client, che funziona sul sistema locale e utilizza profili definiti dall'utente per scaricare in modo proattivo ed automatico aggiornamenti software per la maggior parte dei computer e server Compaq/HP disponibili in commercio.

Per saperne di più su ActiveUpdate, scaricare l'applicazione e creare un profilo personalizzato visitare <http://www.compaq.com/activeupdate>.

Flash della ROM

Il computer è dotato di una flash ROM riprogrammabile. Con la definizione di una password di configurazione in Computer Setup (F10) è possibile proteggere la ROM in modo che non venga involontariamente aggiornata o sovrascritta. Si tratta di un aspetto importante per garantire l'integrità operativa del PC. Dovendo o volendo aggiornare la ROM, è possibile:

- Richiedere alla HP un dischetto con il *ROMPaq*™ aggiornato.
- Scaricare le immagini ROMPaq aggiornate da <http://www.compaq.com>.



ATTENZIONE: Per garantire la massima protezione della ROM, è bene impostare una password di configurazione. La password di impostazione impedisce gli aggiornamenti non autorizzati della ROM. System Software Manager consente all'amministratore di sistema di configurare la password di impostazione su uno o più PC contemporaneamente. Per ulteriori informazioni visitare <http://www.compaq.com/im/ssmwp.html>.

Flash remoto della ROM

Il flash remoto della ROM consente all'amministratore di sistema di aggiornare in condizioni di sicurezza la ROM dei PC HP remoti direttamente dalla consolle di gestione centralizzata della rete. La possibilità per l'amministratore di sistema di eseguire questa operazione a distanza su più PC si traduce in un deployment coerente ed in un maggior controllo delle immagini ROM dei PC HP in rete. Inoltre, ne derivano una maggiore produttività e una diminuzione del costo totale della proprietà.



Per l'esecuzione del flash remoto della ROM, il computer deve essere acceso o attivato tramite Apri sessione remoto.

Per ulteriori informazioni sul flash remoto della ROM vedere Altiris eXpress HP/Compaq Client Manager o System Software Manager su <http://www.compaq.com/easydeploy>.

ROM con blocco di avviamento FailSafe

La ROM con blocco di avvio FailSafe consente il ripristino del sistema nel caso, improbabile, che il flash della ROM non dovesse riuscire, ad esempio in seguito ad interruzione dell'alimentazione durante l'aggiornamento della ROM. Il blocco dell'avvio è una sezione della ROM con protezione flash che effettua un controllo di convalida della ROM ogni volta che il sistema viene acceso.

- Se la ROM di sistema è valida, il sistema parte normalmente.
- Se la ROM di sistema non supera il controllo di convalida, la ROM con blocco di avvio FailSafe fornisce supporto sufficiente per l'avvio del sistema da un dischetto ROMPaq che programmi la ROM con un'immagine valida.

Quando il blocco di avvio rileva una ROM non valida, il sistema emette una serie di segnali acustici (uno lungo e tre brevi), mentre le tre spie della tastiera lampeggiano due volte. A video appare un messaggio che indica la modalità di ripristino del blocco di avvio (su alcuni modelli).

Per ripristinare il sistema in modalità di recovery blocco di avvio procedere come di seguito indicato:

1. Rimuovere gli eventuali dischetti dal lettore e spegnere il sistema.
2. Inserire un dischetto ROMPaq nel lettore.
3. Accendere il sistema.
4. Se non viene rilevato alcun dischetto ROMPaq il sistema ne richiede l'introduzione ed il riavvio del computer.
5. Se è stata impostata una password di configurazione la spia del blocco delle maiuscole si accende ed il sistema richiede l'inserimento della password.
6. Digitare la password di configurazione.
7. Se il sistema riesce ad avviarsi dal dischetto e a riprogrammare la ROM, le tre spie della tastiera si accendono. Il successo dell'operazione viene segnalata inoltre da una serie di segnali acustici di tono crescente.


Per verificare che il flash della ROM è riuscito procedere come di seguito indicato:

1. Inserire un dischetto ROMPaq valido nell'unità a dischetti.
2. Spegnerne il sistema.
3. Riaccendere il sistema per rieseguire il flash della ROM.
4. Se il flash della ROM riesce, tutti e tre i LED della tastiera si accendono e viene emessa una serie di segnali acustici a toni crescenti.
5. Togliere il dischetto, spegnere e riaccendere il computer.

La seguente tabella elenca le diverse combinazioni delle spie della tastiera utilizzate dalla ROM con blocco dell'avviamento con i relativi significati e procedure.

Combinazioni delle spie della tastiera utilizzate dalla ROM con blocco di avvio

Modalità blocco di avvio FailSafe	Colore del LED della tastiera	Tastiera Attività dei LED	Stato/Messaggio
BlocNum	Verde	Acceso	Dischetto ROMPaq non presente, danneggiato o non pronto.*
BlocMaiusc	Verde	Acceso	Immettere la password.*
Bloc Num, Maiusc, Scorr	Verde	Si accendono e si spengono 2 volte (accompagnati da 1 segnale acustico lungo e 3 brevi)	Il flash della ROM è fallito.*
Bloc Num, Maiusc, Scorr	Verde	Acceso	Flash della ROM con blocco dell'avvio eseguito con successo. Spegnerne e riaccendere.

 Le spie diagnostiche non lampeggiano su tastiere USB.

Replica delle impostazioni

Questa procedura offre all'amministratore di sistema la possibilità di copiare facilmente le impostazioni di un computer su altri computer dello stesso modello. Ciò consente una configurazione più veloce e uniforme di più computer. Per replicare le impostazioni:

1. Accedere al menu Utility di Computer Setup (F10).
2. Scegliere **File > Salva su dischetto**. Seguire le istruzioni visualizzate sullo schermo.



Sono necessarie un'unità a dischetti interna o una esterna, portatile.

3. Per duplicare la configurazione, scegliere **File > Ripristina da dischetto** e seguire le istruzioni a video.

Altiris eXpress, System Software Manager e PC Transplant facilitano la replicazione della configurazione e delle impostazioni personalizzate di un PC copiandole su uno o più PC. Per maggiori informazioni visitare <http://www.compaq.com/easydeploy>.

Pulsante d'accensione bistabile

Con le funzioni Advanced Configuration and Power Interface (ACPI) abilitate in Windows 98, Windows 2000, Windows Millennium e Windows XP, il pulsante può funzionare come interruttore di accensione o come interruttore di sospensione. La funzione di sospensione non interrompe completamente l'alimentazione, ma fa entrare il computer in una modalità di minimo consumo energetico. In tal modo è possibile spegnere velocemente il computer senza chiudere le applicazioni e ritornare altrettanto velocemente allo stesso stato operativo senza alcuna perdita di dati.

Per cambiare la configurazione del pulsante di accensione procedere come segue:

1. In Windows 2000, fare clic sul pulsante **Start** e selezionare **Impostazioni > Pannello di controllo > Opzioni risparmio energia**.

In Windows XP, fare clic sul pulsante **Start** e selezionare **Pannello di controllo > Prestazioni e manutenzione > Opzioni risparmio energia**.

2. In **Proprietà – Opzioni risparmio energia** selezionare la scheda **Avanzate**.
3. Nella sezione Pulsanti di alimentazione selezionare l'impostazione del pulsante di alimentazione.

Dopo aver configurato il pulsante di accensione come pulsante di standby, premerlo per portare il sistema ad uno stato di alimentazione ridotta (sospensione). Premere di nuovo il pulsante per riportare rapidamente il sistema dallo standby allo stato di piena alimentazione. Per interrompere completamente l'alimentazione al sistema, premere e tenere premuto il pulsante di accensione per quattro secondi.

Gestione dell'alimentazione

La funzione di Gestione dell'alimentazione interrompe l'alimentazione a determinati componenti del computer quando questi non vengono utilizzati, in modo da risparmiare energia senza che sia necessario spegnere il computer.

Con le funzioni Advanced Configuration and Power Interface (ACPI) abilitate in Windows 98, Windows 2000, Windows Millennium e Windows XP, timeout (il periodo di inattività consentito prima della chiusura di questi componenti) può essere abilitato, personalizzato o disabilitato dal sistema operativo.

1. In Windows 2000, fare clic sul pulsante **Start** e selezionare **Impostazioni > Pannello di controllo > Opzioni risparmio energia**.
In Windows XP, fare clic sul pulsante **Start** e selezionare **Pannello di controllo > Prestazioni e manutenzione > Opzioni risparmio energia**.
2. In **Proprietà – Opzioni risparmio energia** selezionare la scheda **Combinazioni risparmio energia**.
3. Selezionare la combinazione preferita.

Per definire, modificare o disattivare le impostazioni della Gestione dell'alimentazione per quanto riguarda il monitor, occorre utilizzare Proprietà schermo. Per accedervi, è sufficiente fare clic con il pulsante destro del mouse sul **desktop di Windows** e scegliere **Proprietà**.

Sito World Wide Web

I tecnici HP controllano rigorosamente e mettono a punto il software prodotto da HP e da altri fornitori e sviluppano software di supporto specifici per i sistemi operativi, per garantire il massimo del livello di prestazioni, compatibilità e affidabilità dei personal computer HP.

Quando si passa a sistemi operativi nuovi o modificati, è importante implementare il software di supporto creato per il sistema operativo. Se si prevede di utilizzare una versione di Microsoft Windows diversa da quella preinstallata è necessario installare i driver HP corrispondenti e le utility necessarie per garantire il corretto funzionamento.

La HP ha reso più facile il compito di localizzare, accedere, valutare e installare il software di supporto più recente. Scaricare il software da <http://www.compaq.com>.

Il sito contiene gli aggiornamenti ai driver, alle utility ed alle immagini ROM aggiornabili mediante flash, occorrenti per eseguire i sistemi operativi Microsoft Windows sui computer HP.

Moduli e collaboratori

Le soluzioni di gestione HP si basano su standard di mercato, tra cui DMI 2.0, Web-Based Enterprise Management, Intel's Wired for Management (WfM), SNMP e tecnologie PXE. Microsoft, Intel, Altiris ed altre case produttrici di primaria importanza lavorano a stretto contatto con HP per integrare le proprie soluzioni di gestione con i prodotti e le iniziative HP tese a fornire ai clienti HP soluzioni di Intelligent Manageability avanzate per personal systems. Per ulteriori informazioni visitare <http://www.compaq.com/easydeploy>.

Interfaccia di gestione del desktop (DMI)

La Desktop Management Task Force (DMTF) è un ente creato nel 1992 allo scopo di standardizzare la gestione dei sistemi. La DMTF ha definito la struttura della Desktop Management Interface (DMI) per standardizzare l'accesso ai dati di configurazione del PC. HP, in qualità di membro dei comitati Direttivo e Tecnico della DMTF, produce hardware e software compatibili con lo standard DMI.

Per ulteriori informazioni sulla configurazione del software DMI, consultare il file della guida *Intelligent Manageability Guide*.

Wired for Management

L'iniziativa Wired for Management di Intel è mirata a ridurre i costi di assistenza e di amministrazione dei sistemi con architettura Intel senza comprometterne la flessibilità e le prestazioni. Le direttive Wired for Management costituiscono una serie di elementi costruttivi utilizzati da HP in Intelligent Manageability per assicurare una gestione standardizzata degli inventari dei desktop, la configurazione remota dei sistemi, la manutenzione fuori orario e la gestione dell'alimentazione della prossima generazione. Ma HP non si ferma a queste funzioni di base. In Intelligent Manageability sono state implementate ulteriori funzionalità al fine di offrire una soluzione complessiva di gestione di ambienti di rete aziendali.

Le tecnologie Wired for Management includono:

- Desktop Management Interface (DMI) 2.0
- Installazione remota del sistema
- Apri sessione e Chiudi sessione remoti
- Hardware pronto per l'ACPI
- SMBIOS
- Supporto PXE (Pre-boot Execution)

Controllo e sicurezza delle risorse

Le funzioni di AssetControl della Compaq integrate nei PC forniscono dati di controllo sulle principali risorse gestibili con prodotti HP Insight Manager e Management Solutions Partners. L'integrazione automatica e perfetta tra le funzioni AssetControl e questi prodotti consente di scegliere lo strumento di gestione che meglio si adatta al proprio ambiente e che consente di sfruttare al massimo l'investimento in termini di strumenti già esistenti.

I computer HP sono prodotti con l'hardware e il firmware necessari per supportare completamente lo standard DMI 2.0.

HP offre inoltre diverse soluzioni per il controllo dell'accesso ai componenti e ai dati critici del computer. Le funzioni di sicurezza come il sensore e la chiusura Smart Cover, disponibili su alcuni modelli, impediscono l'accesso non autorizzato ai componenti interni del personal computer. Disabilitando le porte parallela, seriale oppure USB, o disabilitando la funzione d'avvio da supporto rimovibile è possibile proteggere risorse dati preziose. Gli allarmi di modifica alla memoria e quelli trasmessi dal sensore Smart Cover possono essere inoltrati automaticamente ai prodotti HP Insight Manager per fornire un'efficace segnalazione dei tentativi di manomissione dei componenti.



Smart Cover Sensor e Smart Cover Lock sono disponibili come opzioni su determinati sistemi.

Per gestire le impostazioni di sicurezza dei computer HP procedere come di seguito indicato:

- In loco, utilizzando le utility di Computer Setup della HP. Per ulteriori informazioni sull'uso delle utility Computer Setup vedere la *Guida all'utility Computer Setup (F10)* in dotazione al computer.
- A distanza, utilizzare System Software Manager. Questo software consente un'installazione sicura e ottimizzata e di controllare le impostazioni di sicurezza con una semplice utility da eseguire dalla riga di comando.

La tabella e le sezioni seguenti si riferiscono alla gestione delle caratteristiche di sicurezza del computer a livello locale tramite le utility Computer Setup (F10).

Descrizione generale delle funzioni di sicurezza

Funzione	Scopo	Come viene attivata
Controllo avvio dispositivi rimovibili	Impedisce l'avviamento da unità a supporti rimovibili.	Dal menu Utility di Computer Setup (F10).
Serial, Parallel, USB, or Infrared Interface Control (Controllo interfaccia seriale, parallela, USB o infrarossi)	Impedisce il trasferimento di dati tramite le interfacce seriali, parallele, USB (universal serial bus) o a infrarossi.	Dal menu Utility di Computer Setup (F10).
Power-On Password (Password d'accensione)	Impedisce l'uso del computer finché non viene immessa la password. Ciò vale sia per l'avvio iniziale che per le operazioni di riavvio.	Dal menu Utility di Computer Setup (F10).
Setup Password (Password di impostazione)	Impedisce la riconfigurazione del computer (uso delle utility di Computer Setup) finché non viene immessa la password.	Dal menu Utility di Computer Setup (F10).
Modalità server di rete	Mette a disposizione funzioni di sicurezza speciali per i computer utilizzati come server.	Dal menu Utility di Computer Setup (F10).
DriveLock	Impedisce l'accesso non autorizzato ai dati su dischi fissi specifici. Questa funzione è disponibile solo su alcuni modelli.	Dal menu Utility di Computer Setup (F10).

Descrizione generale delle funzioni di sicurezza *(Continuazione)*

Funzione	Scopo	Come viene attivata
Sensore Smart Cover	Indica che il coperchio o il pannello laterale del computer sono stati rimossi. È possibile impostarlo in modo che venga richiesta la password di configurazione per il riavvio del computer, dopo la rimozione del coperchio o del pannello laterale. Per ulteriori informazioni su questa funzione consultare la <i>Guida di riferimento hardware</i> sul CDDocumentation Library.	Dal menu Utility di Computer Setup (F10).
Master Boot Record Security (Sicurezza MBR)	Serve per impedire che il Master Boot Record del disco d'avvio venga modificato inavvertitamente o dolosamente e per ripristinare l'ultimo MBR valido.	Dal menu Utility di Computer Setup (F10).
Memory Change Alerts (Allarmi di variazione memoria)	Rileva l'aggiunta, lo spostamento o la rimozione di moduli di memoria, informandone l'utente finale e l'amministratore del sistema.	Per informazioni sull'abilitazione degli allarmi di modifica alla memoria consultare la guida in linea <i>Intelligent Manageability Guide</i> .
Ownership Tag (Contrassegno proprietà)	Durante l'avvio del sistema (protetto da password di configurazione), visualizza le informazioni relative alla proprietà, come definite dall'amministratore del sistema.	Dal menu Utility di Computer Setup (F10).

Descrizione generale delle funzioni di sicurezza (Continuazione)

Funzione	Scopo	Come viene attivata
Cable Lock Provision (Predisposizione per chiusura con cavo)	Impedisce l'accesso all'interno del computer per impedire modifiche non autorizzate della configurazione o la rimozione di componenti. È possibile utilizzarla anche per fissare il computer ad un oggetto immobile, in modo da impedirne il furto.	Utilizzare una chiusura con cavo per assicurare il computer ad un oggetto fisso.
Security Loop Provision (Chiusura di sicurezza)	Impedisce l'accesso all'interno del computer per impedire modifiche non autorizzate della configurazione o la rimozione di componenti.	Installare un lucchetto nella chiusura di sicurezza per impedire modifiche non autorizzate della configurazione o la rimozione di componenti.



Per ulteriori informazioni su Computer Setup vedere la *Guida all'utilità Computer Setup (F10)*.
Il supporto delle funzioni di sicurezza può variare a seconda della configurazione del computer.

Sicurezza tramite password

La password di accensione impedisce l'utilizzo non autorizzato del computer richiedendo l'immissione di una password per accedere alle applicazioni o ai dati ogni volta che il computer viene acceso o riavviato. La password di impostazione impedisce in modo specifico l'accesso non autorizzato a Computer Setup, e può anche essere utilizzata per escludere la password di accensione. Ciò significa che, quando viene richiesta la password di accensione, è possibile accedere al computer anche immettendo la password di configurazione.

È possibile impostare un'unica password per l'intera rete, al fine di consentire all'amministratore della rete di accedere a tutti i sistemi della rete per eseguire le operazioni di manutenzione senza conoscerne la password di accensione, nel caso ne sia stata attivata una.

Impostazione di una password di configurazione tramite Computer Setup

Se si imposta una password di configurazione tramite Computer Setup, si impedisce la riconfigurazione del computer (uso dell'utility di Computer Setup (F10)) finché non viene immessa la password.

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start/Avvio > Chiudi sessione > Riavvia il sistema**.
2. Quando nell'angolo in basso a destra dello schermo viene visualizzato il messaggio di F10 Setup, premere il tasto **F10**. Se necessario, premere **Invio** per saltare la schermata del titolo.



Se non si preme **F10** mentre il messaggio è visualizzato, si dovrà riavviare il computer e poi riaccenderlo per accedere all'utility.

3. Selezionare **Security (Sicurezza)**, quindi **Setup Password (Password di configurazione)** e seguire le istruzioni a video.
4. Prima di uscire scegliere **File > Salva modifiche ed esci**.

Impostazione di una password di accensione tramite Computer Setup

Impostando una password di accensione in Computer Setup si impedisce l'accesso al computer all'accensione, finché non viene immessa la password. Se è stata impostata la password di accensione, Computer Setup presenta le opzioni disponibili (Password Options) nel menu Security (Sicurezza). Le opzioni disponibili sono Network Server Mode (Modalità server di rete) e Password Prompt on Warm Boot (Richiesta password al riavvio).

Se l'opzione Network Server Mode è disabilitata, la password dev'essere immessa ogni volta che si accende il computer o quando sul monitor appare l'icona della chiave. Se l'opzione Password Prompt on Warm Boot è abilitata, la password dev'essere immessa ogni volta che il computer viene riavviato. Se l'opzione Network Server Mode è abilitata, la richiesta della password non viene presentata durante la fase di POST, ma le eventuali tastiere PS/2 restano bloccate fino a quando l'utente non immette la password di accensione.

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start/Avvio > Chiudi sessione > Riavvia il sistema**.
2. Quando nell'angolo in basso a destra dello schermo viene visualizzato il messaggio di F10 Setup, premere il tasto **F10**.
Se necessario, premere **Invio** per saltare la schermata del titolo.



Se non si preme **F10** mentre il messaggio è visualizzato, si dovrà riavviare il computer e poi riaccenderlo per accedere all'utility.

3. Selezionare **Security (Sicurezza)**, quindi **Power-On Password (Password di accensione)** e seguire le istruzioni a video.
4. Prima di uscire scegliere **File > Salva modifiche ed esci**.

Immissione della password di accensione

Per immettere la password di accensione procedere come di seguito indicato:

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start/Avvio > Chiudi sessione > Riavvia il sistema**.
2. Quando viene visualizzata sul monitor l'icona della chiave, digitare la password attuale e premere **Invio**.



Digitare la password con attenzione; per motivi di sicurezza, i caratteri digitati non vengono visualizzati sullo schermo.

Se si immette la password in modo errato, viene visualizzata un'icona di chiave spezzata. Tentare di nuovo. Dopo tre tentativi falliti, è necessario spegnere il computer e riaccenderlo, prima di poter continuare.

Immissione di una password di impostazione

Se sul PC è stata impostata la password di configurazione, ne viene richiesta l'immissione ogni volta che viene eseguito Computer Setup.

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start/Avvio > Chiudi sessione > Riavvia il sistema**.
2. Quando nell'angolo in basso a destra dello schermo viene visualizzato il messaggio di F10 Setup, premere il tasto **F10**.



Se non si preme **F10** mentre il messaggio è visualizzato, si dovrà riavviare il computer e poi riaccenderlo per accedere all'utility.

3. Quando viene visualizzata sul monitor l'icona della chiave, digitare la password di impostazione e premere il tasto **Invio**.



Digitare la password con attenzione; per motivi di sicurezza, i caratteri digitati non vengono visualizzati sullo schermo.

Se si immette la password in modo errato, viene visualizzata un'icona di chiave spezzata. Tentare di nuovo. Dopo tre tentativi falliti, è necessario spegnere il computer e riaccenderlo, prima di poter continuare.

Modifica delle password di accensione e di configurazione

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start/Avvio > Chiudi sessione > Riavvia il sistema**. Per cambiare la password di configurazione, eseguire **Computer Setup**.
2. Quando viene visualizzata l'icona della chiave, digitare la password, una barra (/) o un carattere delimitatore alternativo, la nuova password, un'altra barra (/) o un carattere delimitatore alternativo e ancora la nuova password, come di seguito precisato: **password attuale/nuova password/nuova password**



Digitare la password con attenzione; per motivi di sicurezza, i caratteri digitati non vengono visualizzati sullo schermo.

3. Premere il tasto **Invio**.

La nuova password sarà in vigore a partire dalla prossima volta che si accende il computer.



Per informazioni sui caratteri delimitatori alternativi consultare la sezione di questo capitolo “Caratteri delimitatori delle tastiere nazionali”. Le password d'accensione e di configurazione possono essere modificate anche con le opzioni di sicurezza di Computer Setup.

Cancellazione delle password di accensione e di configurazione

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start/Avvio > Chiudi sessione > Riavvia il sistema**. Per cancellare la password di configurazione, eseguire **Computer Setup**.
2. Quando viene visualizzata l'icona della chiave, digitare la password attuale seguita da una barra (/) o da un carattere delimitatore alternativo, come qui illustrato:
password attuale/
3. Premere il tasto **Invio**.



Per informazioni sui caratteri delimitatori alternativi consultare la sezione “Caratteri delimitatori delle tastiere nazionali”. È possibile modificare la password di accensione e di impostazione anche utilizzando le opzioni di sicurezza di Computer Setup.

Caratteri delimitatori delle tastiere nazionali

Ciascuna tastiera è concepita per soddisfare i requisiti specifici dei singoli paesi. La sintassi e i tasti per la modifica o la cancellazione delle password dipendono dalla tastiera utilizzata.

Caratteri delimitatori delle tastiere nazionali

Araba	/	Greca	–	Russa	/
Belga	=	Ebraica	.	Slovacca	–
BHCSY*	–	Ungherese	–	Spagnola	–
Brasiliana	/	Italiana	–	Svedese/Finnica	/
Cinese	/	Giapponese	/	Svizzera	–
Ceca	–	Coreana	/	Taiwanese	/
Danese	–	Latino-americana	–	Tailandese	/
Francese	!	Norvegese	–	Turca	.
Canadese francofona	é	Polacca	–	Inglese del RU	/
Tedesca	–	Portoghese	–	Inglese degli USA	/

*Per Bosnia-Erzegovina, Croazia, Slovenia e Jugoslavia

Annullamento password

Se si dimentica la password, non è possibile accedere al computer. Per le istruzioni su come eliminare le password consultare la *Guida alla soluzione dei problemi*.

Modalità server di rete

La modalità server di rete (Network Server Mode) prevede alcune funzioni di sicurezza speciali per i computer utilizzati come server. È disponibile solo quando in Computer Setup è stata impostata una password di accensione. Quando è abilitata l'opzione Network Server Mode, la password di accensione non serve per avviare il disco fisso, e non è necessaria la presenza della tastiera. Se è presente una tastiera PS/2, la stessa resta bloccata fino a quanto non viene immessa la password di accensione. Se è presente una tastiera USB, come impostazione predefinita la stessa rimane utilizzabile. Per impedire l'accesso alla tastiera USB dopo che è stato avviato il sistema operativo è necessario nascondere la porta USB tramite l'opzione Device Security (Sicurezza periferiche) del menu Security (Sicurezza) di Computer Setup. Utilizzata in abbinamento all'opzione di accensione After Power Loss (Riavvio dopo interruzione di corrente) di Computer Setup, la funzione Network Server Mode consente il riavvio automatico del server dopo un'interruzione di corrente senza bisogno dell'intervento dell'operatore. Quando è abilitata la funzione Network Server Mode è necessario immettere la password di accensione per avviare i supporti rimovibili (es. dischetti) o le periferiche rimovibili (es. periferiche flash USB).

DriveLock

DriveLock è una funzione di sicurezza che impedisce l'accesso non autorizzato ai dati memorizzati su determinati dischi fissi. DriveLock è stato implementato come estensione di Computer Setup ed è disponibile solo su alcuni sistemi a condizione che utilizzino dischi fissi compatibili.

DriveLock è destinato a clienti HP per i quali la sicurezza dei dati è fondamentale. Per tali clienti il costo del disco fisso e la perdita dei dati archiviati hanno un'importanza secondaria rispetto al danno provocato da un accesso non autorizzato al contenuto. Per bilanciare questo livello di sicurezza con l'esigenza pratica di consentire l'accesso in caso di smarrimento della password, DriveLock utilizza uno schema di sicurezza a doppia password: una dev'essere impostata ed utilizzata da un amministratore di sistema, mentre l'altra viene normalmente impostata ed utilizzata dall'utente finale. Non sono previsti accorgimenti per sbloccare il disco se vengono dimenticate entrambe le password. Pertanto, DriveLock risulta maggiormente indicato quando i dati contenuti sul disco fisso vengono replicati su un sistema informatico aziendale o quando ne viene effettuato il backup su base regolare.

Se entrambe le password di DriveLock vengono smarrite, il disco fisso viene reso inutilizzabile. Per gli utenti che non rispondono ai criteri sopra delineati questo può essere un rischio inaccettabile. Per quelli, invece, che rispondono a tali criteri, il rischio può essere tollerabile, data la natura dei dati memorizzati sul disco.

Uso di DriveLock

L'opzione DriveLock è disponibile nel menu Security (Sicurezza) di Computer Setup. L'utente ha la possibilità di impostare la password principale o di abilitare DriveLock. Per abilitare DriveLock dev'essere specificata una password utente. Dal momento che la configurazione iniziale di DriveLock viene normalmente eseguita da un amministratore di sistema, dev'essere prima di tutto impostata la password principale. HP invita gli amministratori di sistema ad impostare una password principale sia che prevedano di abilitare DriveLock, sia che prevedano di non abilitarlo. In tal modo gli amministratori avranno la possibilità di modificare le impostazioni di DriveLock se si deciderà di bloccare il disco in un secondo tempo. Una volta impostata la password principale l'amministratore di sistema potrà abilitare o meno DriveLock.

Se è presente un disco fisso bloccato, durante il POST chiede la password per sbloccarlo. Se viene impostata una password di accensione e la stessa coincide con quella dell'utente della periferica, durante il POST non viene richiesto all'utente di reimmettere la password. Altrimenti, all'utente viene richiesto di immettere la password per accedere a DriveLock. È possibile utilizzare a tal fine la password principale o quella dell'utente. Gli utenti hanno a disposizione due tentativi per immettere la password corretta. Se entrambi non riescono, il POST prosegue ma i dati sul disco restano inaccessibili.

Applicazioni di DriveLock

La condizione più indicata per la funzione di sicurezza DriveLock è in ambito aziendale, quando un amministratore di sistema fornisce agli utenti dischi fissi multibay da utilizzare in alcuni computer. L'amministratore di sistema è responsabile della configurazione del disco fisso multibay che comporta, tra l'altro, l'impostazione della password principale di DriveLock. Se l'utente dimentica la sua password o la macchina passa ad un altro impiegato, è possibile utilizzare la password principale per cambiare la password utente e riaccedere al disco.

HP consiglia agli amministratori dei sistemi aziendali che decidono di abilitare DriveLock di definire una politica aziendale per l'impostazione e il mantenimento delle password principali. Questa operazione ha lo scopo d'impedire che un dipendente, prima di lasciare l'azienda, imposti intenzionalmente o casualmente entrambe le password di DriveLock. In una simile eventualità il disco fisso non potrebbe più essere utilizzato e dovrebbe essere sostituito. Analogamente, non impostando la password principale gli amministratori di sistema potrebbero vedersi impedito l'accesso al disco per eseguire i controlli di routine del software non autorizzato, altre funzioni di controllo risorse e di supporto.

Per utenti con esigenze di sicurezza meno rigide HP sconsiglia di abilitare DriveLock. Appartengono a questa tipologia singoli utenti ed utenti che conservano dati non importanti sui dischi fissi. Per questi utenti il rischio di perdere il disco in caso di smarrimento di entrambe le password è decisamente superiore al valore dei dati che DriveLock dovrebbe proteggere. L'accesso a Computer Setup e a DriveLock può essere limitato tramite la password di configurazione. Specificando la password di configurazione senza comunicarla agli utenti, gli amministratori di sistema possono impedire loro di abilitare DriveLock.

Sensore Smart Cover

Il sensore Smart Cover, disponibile su alcuni modelli, è una combinazione di tecnologia hardware e software in grado di segnalare se il coperchio o il pannello laterale del computer sono stati tolti. Esistono tre livelli di protezione, come risulta dalla seguente tabella:

Livelli di protezione del sensore Smart Cover

Livello	Impostazione	Descrizione
Livello 0	Disattivato	Il sensore Smart Cover è disattivato (impostazione predefinita).
Livello 1	Notifica all'utente	Quando il computer viene riavviato, sullo schermo viene visualizzato un messaggio che avverte che il coperchio o il pannello laterale del computer sono stati rimossi.
Livello 2	Setup Password (Password di impostazione)	Quando il computer viene riavviato, sullo schermo viene visualizzato un messaggio che avverte che il coperchio o il pannello laterale del computer sono stati rimossi. Per continuare, è necessario immettere la password di impostazione.



Le impostazioni possono essere modificate tramite Computer Setup. Per ulteriori informazioni su Computer Setup vedere la *Guida all'utilità Computer Setup (F10)*.

Impostazione del livello di protezione del sensore Smart Cover

Per impostare il livello di protezione del sensore Smart Cover procedere come di seguito indicato:

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start/Avvio > Chiudi sessione > Riavvia il sistema**.
2. Quando nell'angolo in basso a destra dello schermo viene visualizzato il messaggio di F10 Setup, premere il tasto **F10**. Se necessario, premere **Invio** per saltare la schermata del titolo.



Se non si preme **F10** mentre il messaggio è visualizzato, si dovrà riavviare il computer e poi riaccenderlo per accedere all'utility.

3. Selezionare **Security (Sicurezza)**, quindi **Smart Cover** e seguire le istruzioni a video.
4. Prima di uscire scegliere **File > Salva modifiche ed esci**.

chiusura Smart Cover

Il lucchetto Smart Cover è una chiusura a controllo informatizzato, presente su alcuni computer HP. Questo lucchetto impedisce l'accesso non autorizzato ai componenti interni. Alla consegna, i computer hanno la chiusura Smart Cover sbloccata.



ATTENZIONE: Per garantire la massima sicurezza del blocco del coperchio, è bene stabilire una password di impostazione. La password impedisce l'accesso non autorizzato all'utility Computer Setup.



La chiusura Smart Cover è disponibile come opzione su determinati sistemi.

Blocco della chiusura Smart Cover

Per attivare e bloccare la chiusura Smart Cover procedere come di seguito indicato:

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start/Avvio > Chiudi sessione > Riavvia il sistema**.
2. Quando nell'angolo in basso a destra dello schermo viene visualizzato il messaggio di F10 Setup, premere il tasto **F10**. Se necessario, premere **Invio** per saltare la schermata del titolo.



Se non si preme **F10** mentre il messaggio è visualizzato, si dovrà riavviare il computer e poi riaccenderlo per accedere all'utility.

3. Selezionare **Security (Sicurezza)**, quindi **Smart Cover** e l'opzione **Locked (Bloccata)**.
4. Prima di uscire scegliere **File > Salva modifiche ed esci**.

Disattivazione del blocco di Smart Cover

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start/Avvio > Chiudi sessione > Riavvia il sistema**.
2. Quando nell'angolo in basso a destra dello schermo viene visualizzato il messaggio di F10 Setup, premere il tasto **F10**. Se necessario, premere **Invio** per saltare la schermata del titolo.



Se non si preme **F10** mentre il messaggio è visualizzato, si dovrà riavviare il computer e poi riaccenderlo per accedere all'utility.

3. Selezionare **Security (Sicurezza) > Smart Cover > Unlocked (Sbloccato)**.
4. Prima di uscire scegliere **File > Salva modifiche ed esci**.

Uso della chiave FailSafe Smart Cover

Se la chiusura Smart Cover è abilitata e non è possibile immettere la password per disabilitarla, per aprire il coperchio del computer è necessaria la chiave Failsafe di Smart Cover. La chiave è necessaria in tutte le seguenti circostanze:

- Mancanza di corrente
- Guasto all'avvio
- Guasto dei componenti del PC (ad esempio, processore o alimentatore)
- Password dimenticata



ATTENZIONE: La chiave FailSafe di Smart Cover è uno strumento speciale disponibile presso HP. È bene essere previdenti e ordinare la chiave per tempo presso un rivenditore autorizzato o un centro assistenza (codice ordinazione 166527-001 per chiavi fisse o 166527-002 per chiavi a cacciavite).

È possibile procurarsi la chiave FailSafe in diversi modi:

- Contattare il rivenditore o il centro di assistenza autorizzato HP di fiducia.
- Per informazioni sull'ordinazione visitare <http://www.compaq.com>.
- Chiamare il numero di telefono appropriato, riportato nella garanzia.

Per ulteriori informazioni sull'utilizzo della chiave FailSafe di Smart Cover consultare la *Guida di riferimento hardware*.

Master Boot Record Security (Sicurezza MBR)

Il Master Boot Record (MBR) contiene le informazioni necessarie per l'avvio da un disco e l'accesso ai dati ivi memorizzati. La sicurezza del Master Boot Record serve per impedire modifiche involontarie o dolose all'MBR, come quelle provocate da alcuni virus o dall'uso non corretto di alcune utility. Inoltre essa consente di ripristinare l'ultimo MBR valido nel caso in cui, in fase di riavvio del sistema, vengano rilevate modifiche all'MBR.

Per abilitare la protezione MBR procedere come segue:

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start/Avvio > Chiudi sessione > Riavvia il sistema**.
2. Quando nell'angolo in basso a destra dello schermo viene visualizzato il messaggio di F10 Setup, premere il tasto **F10**. Se necessario, premere **Invio** per saltare la schermata del titolo.



Se non si preme **F10** mentre il messaggio è visualizzato, si dovrà riavviare il computer e poi riaccenderlo per accedere all'utility.

3. Selezionare **Security (Sicurezza) > Master Boot Record Security (Sicurezza Master Boot Record) > Enabled (Abilitata)**.
4. Selezionare **Security (Sicurezza) > Save Master Boot Record (Salva Master Boot Record)**.
5. Prima di uscire scegliere **File > Salva modifiche ed esci**.

Quando la protezione MBR è abilitata il BIOS impedisce qualsiasi modifica all'MBR del disco avviabile corrente in MS-DOS o in Modalità provvisoria di Windows.



La maggior parte dei sistemi operativi controlla l'accesso all'MBR del disco avviabile corrente; il BIOS non è in grado d'impedire che vengano apportate modifiche quando il sistema operativo è in funzione.

Ogni volta che il computer viene alimentato o riavviato, il BIOS confronta l'MBR del disco d'avvio corrente con quello memorizzato in precedenza. Se vengono rilevate modifiche e se il disco avviabile corrente è lo stesso da cui è stato memorizzato l'MBR, viene visualizzato il seguente messaggio:

1999 – Master Boot Record has changed (L'MBR è cambiato).

Premere un tasto per accedere a Computer Setup per configurare la protezione MBR.

Una volta in Computer Setup procedere come segue:

- Salvare l'MBR del disco avviabile corrente;
- Ripristinare l'MBR precedentemente memorizzato; oppure
- Disabilitare la funzione di protezione MBR.

È necessario conoscere l'eventuale password di configurazione.

Se vengono rilevate modifiche e se il disco avviabile corrente **non** è lo stesso da cui è stato memorizzato l'MBR viene visualizzato il seguente messaggio:

2000 – Master Boot Record Hard Drive has changed (Il disco fisso con l'MBR è cambiato).

Premere un tasto per accedere a Computer Setup per configurare la protezione MBR.

Una volta in Computer Setup procedere come segue:

- Salvare l'MBR del disco avviabile corrente; oppure
- Disabilitare la funzione di protezione MBR.

È necessario conoscere l'eventuale password di configurazione.

Nell'improbabile eventualità che l'MBR precedentemente salvato si sia danneggiato viene visualizzato il seguente messaggio:

1998 – Master Boot Record has been lost (l'MBR è danneggiato).

Premere un tasto per accedere a Computer Setup per configurare la protezione MBR.

Una volta in Computer Setup procedere come segue:

- Salvare l'MBR del disco avviabile corrente; oppure
- Disabilitare la funzione di protezione MBR.

È necessario conoscere l'eventuale password di configurazione.

Partizionamento e formattazione del disco avviabile corrente

Verificare che la protezione MBR sia disabilitata prima di modificare la partizione o prima di formattare il disco avviabile corrente. Alcune utility disco (FDISK e FORMAT) cercano di aggiornare l'MBR. Se la protezione MBR è abilitata, quando si cambia la partizione o si formatta il disco è possibile che vengano visualizzati messaggi d'errore dall'utility o un avvertimento relativo alla protezione MBR in occasione del successivo riavvio del computer. Per disabilitare la protezione MBR procedere come segue:

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start/Avvio > Chiudi sessione > Riavvia il sistema**.
2. Quando nell'angolo in basso a destra dello schermo viene visualizzato il messaggio di F10 Setup, premere il tasto **F10**. Se necessario, premere **Invio** per saltare la schermata del titolo.



Se non si preme **F10** mentre il messaggio è visualizzato, si dovrà riavviare il computer e poi riaccenderlo per accedere all'utility.

3. Selezionare **Security (Sicurezza) > Master Boot Record Security (Sicurezza Master Boot Record) > Disabled (Disabilitata)**.
4. Prima di uscire scegliere **File > Salva modifiche ed esci**.

Predisposizione per chiusura con cavo

Sul retro del computer è presente la predisposizione per la chiusura con cavo in modo da bloccare fisicamente il computer al piano di lavoro.

Per le istruzioni illustrate consultare la *Guida di riferimento hardware* nel CD *Documentation Library*.

Tecnologia per l'identificazione delle impronte digitali

Eliminando la necessità di immettere le password utente, la tecnologia per il riconoscimento delle impronte digitali della HP migliora la sicurezza della rete, semplificando il processo di accesso e riducendo i costi associati alla gestione delle reti aziendali. Grazie al prezzo accessibile, la funzione non è più appannaggio esclusivo delle organizzazioni high-tech con esigenze di sicurezza elevate.



Il supporto per la tecnologia d'identificazione delle impronte digitali varia da modello a modello.

Per ulteriori informazioni visitare

http://www.compaq.com/products/quickspecs/10690_na/10690_na.html

Notifica guasti e ripristino

Le funzioni di notifica guasti e ripristino combinano hardware innovativo e tecnologia software al fine di prevenire la perdita di dati critici e ridurre al minimo i periodi di inattività non programmati.

Quando si verifica un guasto, il computer visualizza un messaggio di avviso locale che contiene una descrizione del guasto e le procedure consigliate. Tramite HP Insight Management Agent è possibile visualizzare lo stato attuale di integrità del sistema. Se è collegato ad una rete gestita da un prodotto HP Insight Manager o da altri prodotti di Compaq Management Solutions Partner, il computer invia anche un avviso di guasto all'applicazione di gestione della rete.

Drive Protection System (DPS)

Drive Protection System (DPS) è uno strumento di diagnostica incorporato nei dischi fissi installati su alcuni computer HP, progettato per consentire la diagnosi di problemi che potrebbero provocare la sostituzione di dischi fissi non in garanzia.

In fase di produzione dei computer HP, i dischi fissi installati vengono collaudati uno per uno tramite DPS ed in essi viene registrato un record permanente di dati chiave. Ogni volta che viene eseguito il DPS, gli esiti del test vengono scritti sul disco fisso. Il fornitore di servizi potrà servirsi di queste informazioni per diagnosticare le condizioni che hanno indotto l'utente ad eseguire il software DPS. Per le istruzioni sull'uso del DPS consultare la *Guida alla soluzione dei problemi*.

Monitoraggio dell'integrità ultra ata

Il monitoraggio dell'integrità dell'Ultra ATA verifica l'integrità dei dati nel trasferimento tra un disco fisso Ultra ATA e la logica centrale del sistema. Se il computer rileva un numero eccessivo di errori di trasmissione, sullo schermo viene visualizzato un messaggio di allarme locale con l'indicazione delle procedure consigliate.

Alimentatore protetto contro gli sbalzi di tensione

Un alimentatore integrato protetto contro gli sbalzi di tensione garantisce maggiore affidabilità in presenza di instabilità nell'alimentazione. L'alimentatore è concepito per tollerare sbalzi di tensione fino a 2000 volt, senza esporre il sistema a periodi di inattività o perdita di dati.

Sensore termico

Il sensore termico è una funzione hardware e software che controlla la temperatura interna del computer. Quando la temperatura supera i valori normali, questa funzione visualizza un messaggio di allarme che consente di intervenire prima che vengano danneggiati i componenti interni o che si verifichi una perdita di dati.

Indice Analitico

A

- accesso al computer, controllo 15
- ActiveUpdate 7
- aggiornamento ROM 8
- Alimentatore con tolleranza alle
sovratensioni 35
- alimentatore protetto contro gli sbalzi di
tensione 35
- Altiris eXpress 4
- Altiris eXpress HP/Compaq Client Manager
6
- Altiris eXpress PC Transplant Pro 6
- AssetControl 15
- attenzione
 - chiave FailSafe 30
 - protezione della ROM 8
 - sicurezza chiusura coperchio 28

B

- blocco della chiusura Smart Cover 29

C

- cambiamento password 22
- cancellazione password 23
- caratteri delimitatori delle tastiere nazionali
23
- caratteri delimitatori, tabella 23
- chiave FailSafe
 - attenzione 30
 - ordinazione 30
- chiave FailSafe di Smart Cover, ordinazione
30
- chiusura con cavo 34
- chiusura coperchio intelligente 28

- chiusura Smart Cover

 - blocco 29

 - sblocco 29

- configurazione iniziale 2

- configurazione pulsante di accensione 11

- controllo dell'accesso al computer 15

D

- dischi fissi, strumenti diagnostici 35

- dischi, protezione 35

- disco avviabile, informazioni importanti 33

- disco, clonazione 2

- DMI (Desktop Management Interface) 14

E

- eliminazione password 24

F

- Flash remoto della ROM 8

- formattazione dischi, informazioni importanti
33

- funzioni di sicurezza, impostazione 15

- funzioni di sicurezza, tabella 16

G

- Gestione dell'alimentazione 12

I

- immagine software preinstallata 2

- immissione

 - password di accensione 20

 - password di configurazione 21

- impostazione

 - password di accensione 19

 - password di configurazione 19, 21

 - Sensore Smart Cover 28

 - timeout 12

- impostazioni, replicazione 11
- indirizzi Internet, vedere siti Web
- Indirizzi Internet. Vedere Siti Web
- installazione iniziale 2
- installazione remota 3
- Installazione remota del sistema, accesso 3
- integrità dei dati 35
- Intelligent Manageability 14
- Interfaccia di gestione del desktop (DMI) 14

M

- modifiche ai sistemi operativi, informazioni importanti 13
- Monitoraggio dell'integrità ultra ata 35

N

- notifica guasti 34

O

- ordinazione Chiave FailSafe 30

P

- partizione dischi, informazioni importanti 33
- password
 - cancellazione 23
 - d'accensione 20
 - d'accensione 19
 - eliminazione 24
 - installazione 19, 21
 - modifica 22
- password di accensione
 - cancellazione 23
 - immissione 20
 - impostazione 19
 - modifica 22
- password di configurazione
 - cancellazione 23
 - immissione 21
 - impostazione 19
 - modifica 22
- PCN (Product Change Notification) 7

- personalizzazione software 2
- Product Change Notification (PCN) 7
- protezione dei dischi fissi 35
- protezione della ROM, avvertenza 8
- protezione MBR (Master Boot Record) 31
- protezione MBR (Master Boot Record),
 - impostazione 31
- pulsante d'accensione
 - configurazione 11
- pulsante d'accensione
 - bistabile 11
- pulsante di accensione bistabile 11

R

- ripristino del sistema 9
- ripristino software 2
- risparmio energetico 12
- risparmio energetico, impostazioni 12
- ROM con blocco di avviamento FailSafe 9
- ROM di sistema non valida 9
- ROM, aggiornamento 8
- ROM, non valida 9

S

- sblocco della chiusura Smart Cover 29
- Sensore Smart Cover
 - impostazione 28
 - livelli di protezione 27
- Sensore termico 35
- sicurezza chiusura coperchio, avvertenza 28
- sicurezza tramite password 18
- sistemi operativi, informazioni importanti sulla modifica 13
- siti Web
 - www.compaq.com 8, 13, 30
 - www.compaq.com/activeupdate 7
 - www.compaq.com/easydeploy 5, 6, 8, 11, 13
 - www.compaq.com/im/ssmwp.html 7, 8
 - www.compaq.com/pcn 7

- www.compaq.com/products/quickspecs/10690_na/10690_na.html 34
 - www.compaq.com/solutions/pcsolutions 2
 - software
 - aggiornamento di più macchine 7
 - Altiris eXpress 4
 - AssetControl 15
 - Drive Protection System (DPS) 35
 - Flash remoto della ROM 8
 - Gestione dell'alimentazione 12
 - Installazione remota del sistema 3
 - integrazione 2
 - Master Boot Record Security (Sicurezza MBR) 31
 - Notifica guasti e ripristino 34
 - ripristino 2
 - ROM con blocco di avviamento
 - FailSafe 9
 - System Software Manager 7
 - utility Computer Setup 11
 - spie della tastiera, ROM, tabella 10
 - spie ROM della tastiera, tabella 10
 - SSM (System Software Manager) 7
 - strumenti di clonazione, software 2
 - strumenti di installazione, software 2
 - strumenti diagnostici per dischi fissi 35
 - System Software Manager (SSM) 7
- T**
- tecnologia per l'identificazione delle impronte digitali 34
 - tecnologie Wired for Management 14
 - temperatura interna del computer 35
 - timeout, impostazione 12
- U**
- URL (siti Web). Vedere Siti Web
 - utility Computer Setup 11